

SECRET

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/11<sup>1</sup>

SECURITY COMMITTEE

(Effective 23 August 1974)

In support of the DCI's statutory responsibilities and of his efforts to improve the Intelligence Community's product and to achieve more efficient use of intelligence resources, the community's security policies and procedures must be effective and consistent for the protection of intelligence and of intelligence sources and methods,<sup>2</sup> and must ensure timeliness and economy in the handling of compartmented information. Therefore, pursuant to provisions of Subsection 102 (d) of the National Security Act of 1947, as amended, to provisions of NSCID 1 and to paragraph 2.b of NSAM 317, a new standing Committee of the USIB is hereby established.

1. *Name of the Committee*

The committee will be known as the Security Committee.

2. *Mission*

The mission of the committee is to provide the means by which the Director of Central Intelligence, with the advice of United States Intelligence Board principals, can:

a. Ensure establishment of security policies and procedures including recommendations for legislation for the protection of intelligence and intelligence sources and methods from unauthorized disclosure.

b. Review and formulate personnel, physical and document security policies, standards and practices and dissemination procedures applicable to all government departments and agencies as such policies, standards, practices and procedures relate to the protection of intelligence

<sup>1</sup> Supersedes DCID 1/11, effective 23 April 1965 and DCID 1/12 effective 23 December 1964.

<sup>2</sup> The term intelligence as used in this document applies only to information covered by statute, Executive Order, or other authority consonant with the DCI's statutory responsibility for foreign intelligence and for the protection of intelligence and intelligence sources and methods from unauthorized disclosure.

25X1

MORI Search Completed  
MORI #17697  
RIPPUB  
06/29/04

1  
SECRET

Approved For Release 2005/04/22 : CIA-RDP96B01172R000300010012-6

25X1

SECRET

sources and methods in consideration of the effectiveness, risks and cost factors involved.

25X1

c. Review and formulate policies and procedures governing the release of intelligence to foreign governments and international organizations and the review of classified intelligence proposed for release to the public through declassification or other action. With respect to foreign disclosure, ensure that releases are in consonance with U.S. security policy, [redacted] and that the intelligence itself is accorded a degree of protection equal to that afforded by the United States. With respect to public release, ensure that disclosure or declassification actions are taken pursuant to proper authority and that they are accomplished so as to minimize the risk to other intelligence sources and methods.

d. Ensure that appropriate investigations are made of any unauthorized disclosure or compromise of intelligence or of intelligence sources and methods and that the results of such investigations, along with appropriate recommendations, are provided to the Director of Central Intelligence.

e. [redacted]

25X1

f. Review special security and compartmentation procedures and develop proposals for any necessary changes to achieve optimum use of intelligence consistent with protection of sensitive intelligence sources and methods.

g. Ensure the development, review and maintenance of security standards and procedures for the protection of intelligence stored in or processed by computers.

### 3. Functions

The functions of the committee are:

a. To advise and assist the Director of Central Intelligence as appropriate in the development and review of security policies, standards, procedures and practices for the protection of intelligence and intelligence sources and methods from unauthorized disclosures.

b. To review, formulate and recommend to the Director of Central Intelligence policies, standards and procedures for the dissemination of intelligence materials, for the release of such materials to foreign governments, and for the review of classified intelligence proposed for use in unclassified activities.

c. On behalf of the Director of Central Intelligence, to call upon departments and agencies to investigate any unauthorized disclosure or compromise of intelligence or of intelligence sources and methods occurring within their departments and agencies; to report the results

SECRET

25X1

of these investigations to the Director of Central Intelligence, through the United States Intelligence Board. Such reports will (1) assess the disclosure's impact on the U.S. intelligence process, and its implications for national security and foreign relations, (2) describe corrective measures taken or needed to prevent such disclosures in the future or to minimize the adverse effects of the case at hand, and (3) recommend any appropriate additional actions.

25X1 d. The functions of the committee as they relate to [redacted]  
[redacted] computer security and special security compartmentation are set forth in attachments 1, 2, and 3.

#### 4. *Community Responsibilities*

a. Upon request of the committee chairman, USIB departments and agencies shall furnish to the committee within established security safeguards particular information needed by the committee and pertinent to its functions. Temporary material and ad hoc personnel support will be provided to the committee as needed and as mutually agreed upon by the departments and agencies represented on the committee.

b. Each USIB principal is responsible for investigation of any unauthorized disclosure or compromise of intelligence or intelligence sources and methods occurring within his department or agency. When investigation determines that the possibility of compromise cannot be discounted, and the interests of the USIB or another USIB principal are involved or affected, the results of investigation will be forwarded to the Security Committee for review and possible remedial action as determined appropriate by the committee.

#### 5. *Composition and Organization*

a. The committee will consist of a full-time chairman designated by the DCI, representatives of the chiefs of departments and agencies who are members of the USIB, and the representatives of the Departments of the Army, Navy, and Air Force. The chairman may invite a representative of the chief of any other department or agency having functions related to matters being considered by the committee to sit with the committee whenever matters within the purview of that department or agency are to be discussed.

25X1 b. The committee will be supported by [redacted]  
[redacted] subcommittees as needed and as approved by the DCI and by ad hoc working groups as approved by the chairman. The chairman of subcommittees will be designated by the committee chairman with the concurrence of the DCI. Membership on the subcommittees and ad hoc working groups need not be limited to member agencies of the committee, but may be

SECRET

extended by the chairman to representatives of other departments and agencies having related functional responsibilities or support capabilities.

c. The committee will have a full-time support staff to be provided by USIB departments and agencies as arranged and approved by the DCI.

6. *Rules of Procedure*

a. The committee shall meet upon the call of the chairman or at the request of any of its members. Items may be placed on the agenda by the DCI or by the chairman or any member of the committee.

b. Decisions or recommendations will be formulated by the chairman after giving consideration to the views of the members. At the request of a dissenting member, the chairman will refer the decision or recommendation along with dissenting opinion or opinions to the DCI.

W. E. Colby  
Director of Central Intelligence

SECRET

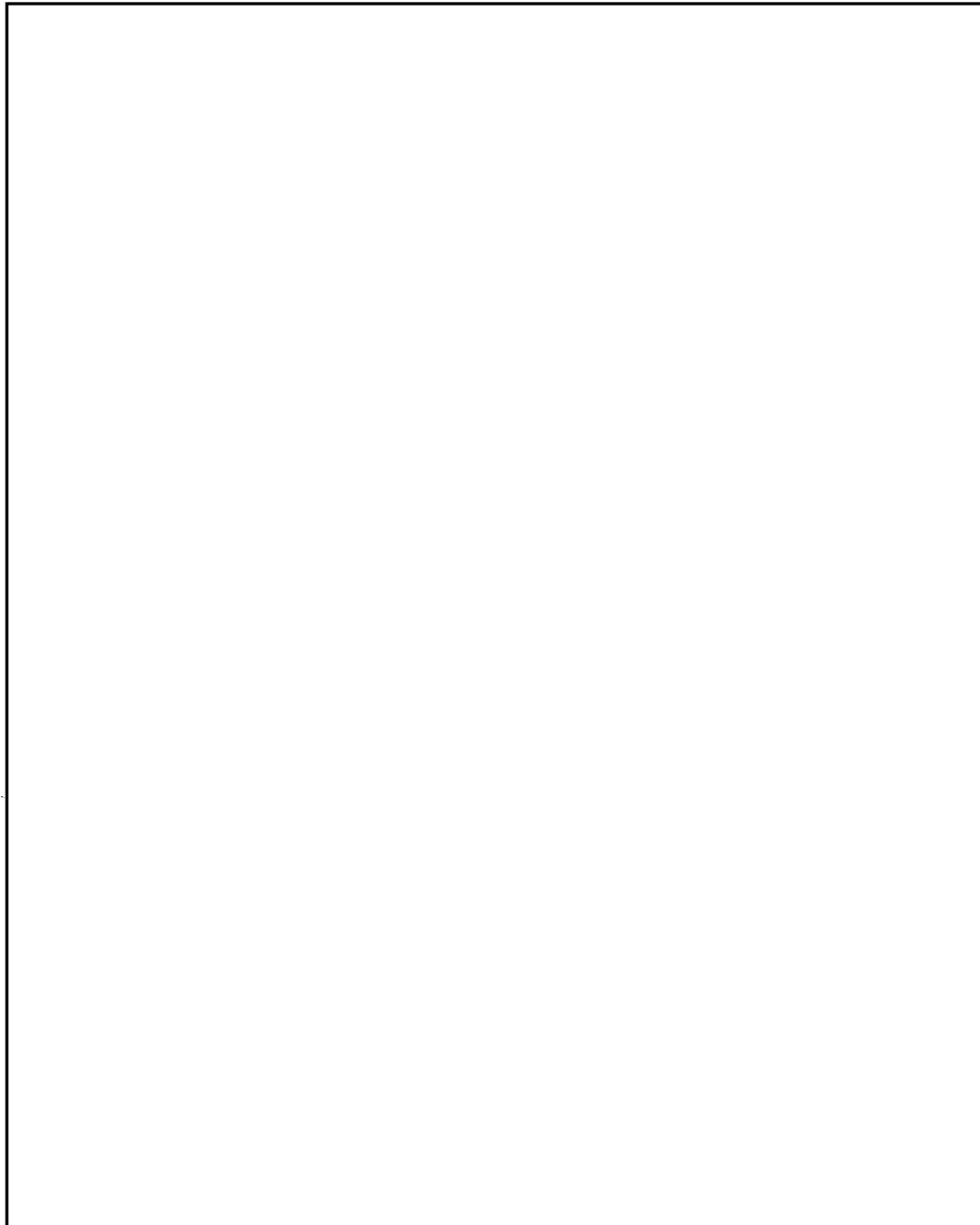
25X1



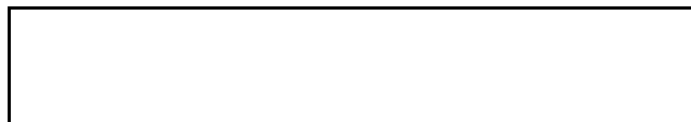
25X1

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/11

(Attachment 1)



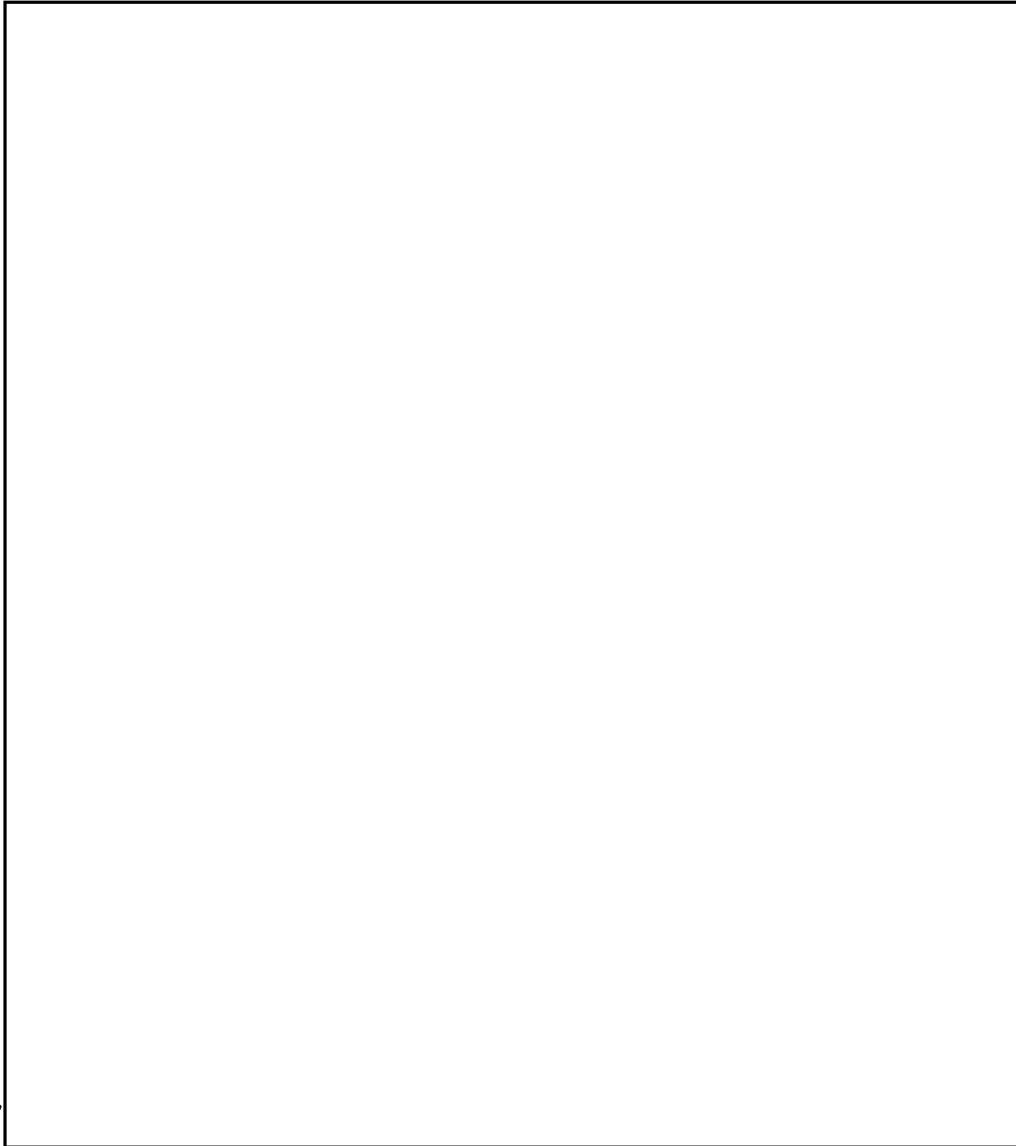
25X1



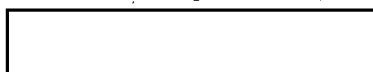
25X1



25X1



25X1



25X1

SECRET

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/11

(Attachment 2)

Computer Security

The functions of the Security Committee include:

(1) To review, formulate and recommend to the DCI policies, standards, and procedures to protect intelligence data stored or processed by computer.

(2) To advise and assist the DCI, the Intelligence Community Staff, Committees of the United States Intelligence Board, USIB member agencies and departments, and other intelligence users with respect to all computer security issues and to resolve conflicts that may arise in connection therewith.

(3) To formulate and recommend to the DCI resource programming objectives for USIB departments and agencies in the field of computer security in consideration of current and foreseen vulnerabilities and threats and with regard for the effective and efficient use of resources; to foster and to monitor an aggressive program of computer security research and development in the Intelligence Community in order to avoid unwarranted duplication and to assure the pursuit of an effective effort at resolving technical problems associated with the protection of computer operations.

(4) To coordinate all aspects of Intelligence Community efforts in defense against hostile penetration of Community computer systems as feasible to support other Government and national efforts aimed at improving computer security technology; to foster a coordinated program of Intelligence Community computer security training and indoctrination.

(5) To facilitate within the Intelligence Community the exchange of information relating to computer security threats, vulnerabilities, and countermeasures by providing a focal point for the evaluation of foreign intentions and capabilities to exploit Community computer operations, for central notification of hostile exploitation attempts, for the preparation of damage assessments of incidents of foreign exploitation of intelligence computer operations, and for the formulation of Community policy on the release of computer security information to foreign governments and international organizations.

7  
SECRET

25X1

Copy No  25X1

(6) To review, formulate and recommend minimum computer security standards, procedures and criteria as guidance for system design, evaluation and certification of acceptable levels of security for computer systems.

FOR ON

SECRETARY OF DEFENSE  
WASHINGTON, D.C. 20301

THE SECRETARY OF DEFENSE  
ATTENTION: DIRECTOR, ARPA  
WASHINGTON, D.C. 20301

THE SECRETARY OF DEFENSE  
ATTENTION: DIRECTOR, ARPA  
WASHINGTON, D.C. 20301  
ATTENTION: DIRECTOR, ARPA  
WASHINGTON, D.C. 20301

THE SECRETARY OF DEFENSE  
ATTENTION: DIRECTOR, ARPA  
WASHINGTON, D.C. 20301  
ATTENTION: DIRECTOR, ARPA  
WASHINGTON, D.C. 20301

THE SECRETARY OF DEFENSE  
ATTENTION: DIRECTOR, ARPA  
WASHINGTON, D.C. 20301  
ATTENTION: DIRECTOR, ARPA  
WASHINGTON, D.C. 20301



SECRET

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/11

(Attachment 3)

Compartmentation<sup>1</sup>

The functions of the Security Committee as they relate to compartmentation controls are:<sup>2</sup>

A. To develop and recommend to the DCI, with the advice of the United States Intelligence Board, technical guidance for the establishment, maintenance and improvement of coordinated compartmentation systems.

(1) Providing special protection to sensitive intelligence, intelligence information and intelligence sources and methods under the authority of Section 9 of Executive Order 11652.

(2) Ensuring the establishment and disestablishment of compartmentation of intelligence and intelligence information on the instructions of the DCI.

(3) Ensuring coherent control by the DCI of the processes for access approvals to compartmented intelligence and intelligence information and of the processes for dissemination, sanitization or release of such intelligence information.

(4) Ensuring the establishment and promulgation or appropriate criteria for security and need-to-know access approvals.

B. To formulate, coordinate, maintain and promulgate technical guidance for use in the administration of compartmentation controls at all echelons of department and agency [redacted] activity, [redacted] concerning:

25X1

(1) Access approval criteria [redacted]

25X1

(2) Physical Security.

<sup>1</sup>The term "compartmentation" as used in this directive refers to the system whereby special Intelligence Community controls indicating restricted handling within collection programs and their end products are applied to certain types of intelligence information and material. The term does not include Restricted Data as defined in Section 11, Atomic Energy Act of 1954, as amended.

25X1

9  
SECRET

25X1

Attachment 3

SECRET

(3) Document identification, handling, accountability and destruction.

(4) Automatic data processing and associated materials.

C. To furnish technical guidance and assistance

25X1

[redacted]  
[redacted] in connection with their sanitization, downgrading, declassification and decontrol responsibilities.

D. To review and survey, when appropriate, with the cooperation and assistance of the USIB Principal concerned, the security standards, practices and procedures employed by USIB departments and agencies [redacted] in relation to approved compartmentation policies, procedures and controls; and to make recommendations for practical improvements to the USIB Principals concerned through the DCI.

25X1

E. [redacted]

25X1

F. To recommend security policies, in coordination with appropriate USIB committees, governing the release or disclosure of compartmented intelligence [redacted]

25X1

25


DIRECTOR OF CENTRAL INTELLIGENCE  
**Security Committee**

SECOM-D-488

2 APR 1979

MEMORANDUM FOR: Security Committee Principals and Observers

STATINTL FROM:

  
Executive Secretary

SUBJECT: Unauthorized Disclosures

1. Security Committee deliberations at the March conference resulted in this subject being selected for priority attention during 1979. The attached memorandum contains a number of proposals for dealing with the subject. With the Chairman's approval, it is forwarded for your consideration.

2. Request that you familiarize yourselves with the attached and come to the 11 April 1979 SECOM meeting prepared to discuss it. This matter will be taken up under new business on the agenda.

  
STATINTL

Attachment

DIRECTOR OF CENTRAL INTELLIGENCE  
**Security Committee**

SECOM-D-479

100-100000

ATINTL

MEMORANDUM FOR: Chairman, DCI Security Committee

FROM:

[Redacted]  
Executive Secretary

SUBJECT: Unauthorized Disclosures

1. This topic was selected by the Security Committee for priority attention during 1979.

2. The following actions are proposed toward this goal.

a. Elevate the Unauthorized Disclosures Working Group to a permanent Subcommittee of the SECOM. Action required:

1. Draft memorandum for signature Chairman to DCI obtaining approval for this action.

2. Necessary charter changes to DCID 1/11.

Comment: The present Chairman of the UDWG has requested relief from this duty on the press of other business.

In recognition that DIA has chaired this activity for over a year it may be advisable to rotate the chair at this time. A considerable number of unauthorized disclosures are reported by NSA. There may be advantage to asking NSA to head this activity.

b. Improve the Leak Data Base.

All reports of leaks should be accomplished by a completed form which will serve to input the computer data base.

c. Establish a point of knowledgeable contact in each member of the NFIB (preferable the Department's representation on the UD Subcommittee. Primarily an action officer.)

d. Reinstitute the concept with the UD Subcommittee of a Fast Reaction Element composed of those members whose agencies may be involved in any given leak. Functions would be to:

1. Determine whether the issue is a leak of NFI.
2. Determine what agencies should be asked to initiate immediate investigation and to task them accordingly.
3. Determine whether there should be a recommendation to the DCI requesting an FBI investigation.
4. Should it be determined that further investigation would be futile or have no salutary effect, cancel various in-house investigations and assure that the leak data base has been updated.

e. Establish a contact in the Criminal Division of the Attorney General's office and the FBI and send copies of each report of leak direct to them.

f. Establish contacts in the Senate and House Intelligence Committees and send them copies of each report of leak through the DCI's office of Legislative Council.

g. Seek DCI agreement to petition the Director FBI and the Attorney General to be more willing to do investigations of Unauthorized Disclosures.

1. Obtain support of NFIB members for campaign.
2. Present concern at an NFIB meeting.
3. Obtain support of NSC.

h. Seek DCI agreement to ask the President for an expression of concern about Unauthorized Disclosures.

i. Start a publicity push to make every NFI member aware that unauthorized disclosures are detrimental.

- Include flyers in each Intel Pub for a week.
- Put out notices to all personnel in each agency.
- For one week, ask everyone who meets with the press to report it, naming the reporter and the subject(s) covered.
- Put notices on bulletin boards, on tables in cafeterias (including the Executive Dining Room).
- Get cable message to use with each cable for one day.
- Get out book dispatch over all network lines - leaving it to communicators to attach copy to distribution lists.

j. Seek DCI support for establishing a small investigative group composed of representatives of the IC that have DCI authority to cross departmental lines in pursuit of resolution of unauthorized disclosures of National Foreign Intelligence.

k. Recognize that there are some "authorized disclosures" and task the Unauthorized Disclosure Subcommittee to work out a mechanism whereby a determination can be made as to the category of leak (i.e., authorized or unauthorized) before investigations are initiated.

3. These proposals are submitted in the belief that they are goal oriented, represent a revitalization of actions and interest within the prerogatives of the Security Committee and will reflect to the NFIB a positive posture by the Committee. Since a major portion of the proposed actions are resource consuming, it is suggested that the Committee pick a period, say the month of June, and a week within that month, perhaps the 2nd week, to devote necessary resources to this effort.

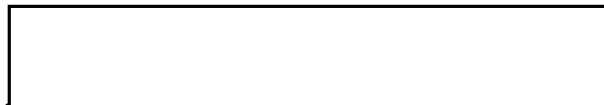
4. With approval of the Chairman this memorandum will be provided to members for consideration and comments.



STATINTL

APPROVED:

STATINTL



Robert W. Gambino  
Chairman  
DCI Security Committee

29 Jan 79  
Date

Distribution:

Orig - Addressee return SECOM

1 - C/SECOM

1 - SECOM Chrono

1 - SECOM Subject

ONLY YOU CAN PREVENT  
THIS MATERIAL FROM BECOMING  
AN UNAUTHORIZED DISCLOSURE.

DO NOT ABUSE THE TRUST THAT  
ACCOMPANIES YOUR ACCESS  
TO THIS AND OTHER U.S. GOVERNMENT  
SENSITIVE INTELLIGENCE.



Further needs on Anti Leak Campaign

1. Revision of DCID 1/11 to incorporate as Attachment a charter for the Unauthorized Disclosures Subcommittee.
2. Designation of CSG member as focal point.
3. Ideas for flyers on table folders cautioning against leaks.
4. Coordination with PI officers in the I.C. and also in House and Senate and OLC+NSC.
5. Means to get this program brought to the attention of each NFIB member through their SECOM member.
6. Preparation of material for C/SECOM to present to NFIB.

(Book a time with Walt Elder.)

7. Paper for C/SECOM to present to the DCI outlining this campaign and seeking his support and approval to present to NFIB.